

3/17/06

Washington State Health Care Authority
Health Information Infrastructure Advisory Board

Preliminary Report on Emergency Access to Electronic Medical Information

Assignment

Collect and summarize information about policies related to emergency ("break the glass") access to electronic medical information that are used when patients are unable to provide consent.

Summary of Preliminary Policy Recommendation

In an emergency situation where it is not possible to obtain patient consent for records access (e.g. the patient is unconscious), a bona fide emergency provider who has been duly authenticated by the system should have immediate access to a patient's electronic health record information, provided that 1) the patient has previously agreed to such emergency access, and 2) an audit record available to the patient is generated.

Background Information

1. Policy from Johns Hopkins (relevant section in *italics*)

Access to E-PHI and to E-PHI Systems shall be allowed only to those workforce members, vendors or software programs that have been granted access rights pursuant to Administrative Security Policy (HIPAA Policy C.2, Section C). Unique user identification and effective user and entity authentication are required for E-PHI Systems.

REQUIREMENTS

1. Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures that include the following access controls:

a. Access control procedures (including authorization, administrator access, authentication, termination and emergency access)

b. Issuance of unique (not shared between multiple users) user ID's with appropriate authentication mechanisms (e.g. passwords, tokens, etc.)

c. Efforts to move from single factor to multi-factor authentication (e.g. biometric, tokens) and to use single sign-on (SSO) for E-PHI Systems

d. Emergency access procedures for users and administrators and responsible individuals designated

e. Procedures for automatic log-off of users after a predetermined time of inactivity.

2. Policy from Inland Northwest Health Services, Spokane (relevant section in *italics*)

This “policy” statement documents Patient Care Inquiry (PCI) computer module access of Emergency Room (ER) Physicians operating throughout the Inland Northwest Health Services/Information Resource Management network (INHS/IRM).

It is the policy of Inland Northwest Health Services that:

All ER Physicians operating in all hospitals supported by the INHS/IRM network have “unrestricted” PCI access.

The above unrestricted PCI access allows ER Physicians access to the medical visit history of any patient of any INHS/IRM supported facility who presents themselves to the ER Physician for treatment.

This access is granted to ER Physicians at the time of initial set-up of the individual ER Physician in PCI and requires no extra-ordinary efforts. *This does not represent a “break-the-glass” type of policy for that reason but rather makes such not necessary.*

3. Policy from Indianapolis Network for Patient Care

No policy is necessary, as patients consent to such access upon enrollment.

4. Recommendation in draft policy from Markle Foundation

"In the event of a health care emergency, some method may be provided to allow access in the event of an authentication failure as a kind of "Break the Glass" function on an existing account. However, role-based authorization is not sufficient for the use of the system; no access to the system should be allowed for any such role without a human identifier attached. It is not enough to ask that someone prove that they have admitting privileges at General Hospital; they must also provide their actual identity, so that should a later audit be required, a person can be associated with the audited actions, not just a role."

Analysis

There appears to be a general view that emergency access to patient electronic records by authorized personnel is essential, provided the individual user's identity is properly authenticated. The patient's prior consent for such emergency access should be obtained and recorded if possible.